PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/60, 1/00

A2

(11) International Publication Number: **WO 98/30964**

(43) International Publication Date: 16 July 1998 (16.07.98)

(21) International Application Number: PCT/SE98/00011

(22) International Filing Date: 9 January 1998 (09.01.98)

(30) Priority Data:
9700063-2 9 January 1997 (09.01.97) SE

(71) Applicant *(for all designated States except US)*: BUYONET INTERNATIONAL [SE/SE]; Eklandagatan 55, S-412 61 Göteborg (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: TENGBERG, Freddy [SE/SE]; Delsjövägen 7, S-412 66 Göteborg (SE).

(74) Agent: GÖTEBORGS PATENTBYRÅ AB; Sjöporten 4, S-417 64 Göteborg (SE).

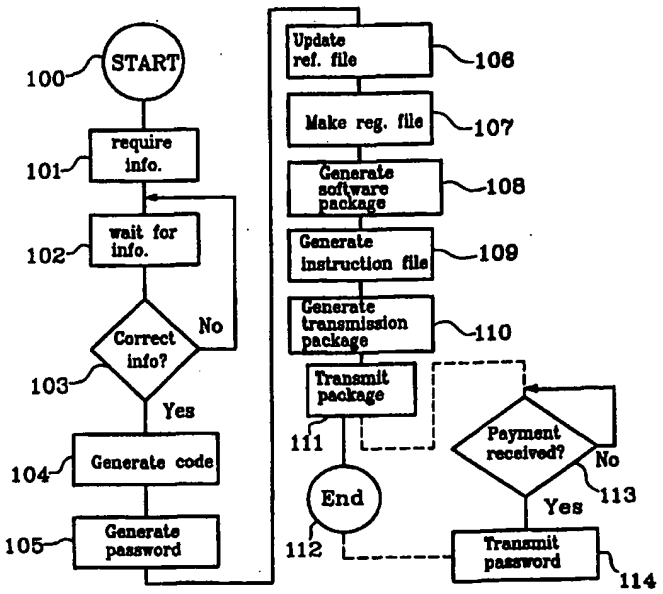
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
In English translation (filed in Swedish).
Without international search report and to be republished upon receipt of that report.

(54) **Title:** A SYSTEM FOR SECURE DATA TRANSMISSION OVER AN ELECTRONIC LINK

(57) **Abstract**

A system for data transmission over an electrical link (12) including at least one distribution server (10) and one client station (11), which requests transmission of a specific data set from a distributor, communicating with the distribution server (10). The server (10) is arranged to produce a first encrypted and with a password-locked package of said specific set of data, the password being generated at least partly based on the information received from the client station (11). The server (10) is provided to produce a second package (24) containing said first package and an instruction set, at least part of the second package being accessible if the client station (11) receives it in its entirety after a transmission. The encrypted set of the data is further provided to be accessed if the client station (11) performs instructions acceptable for the distributor, and supplies the password for unlocking said first package.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A SYSTEM FOR SECURE DATA TRANSMISSION OVER AN ELECTRONIC LINK

Technical field

The invention refers to a system for data transmission over an electrical link including at least one distribution server and one client station, which requests transfer of a specific data set from a distributor communicating with the distribution server.

Background of the invention

There is a major drawback with present software trading "over disk". Most of the softwares are packaged in big and clumsy boxes, with corresponding documentation, which itself requires handling and production costs. Usually, the software passes via many middlemen with corresponding transportation before it reaches the end user, the handling increases the price of the software. The great demand results in that one usually has large software stocks, with resulting capital accumulation. The fast development has resulted in the continues upgrades of the software, which leads to inventory markdowns.

The explosive application of services via the worldwide computer network "Internet", has lately introduced possibilities, which have not been interesting before. Possibility to transfer large amounts of information without intermediate storing has given rise to discussions about trade via the Net, i.e. marketing of, for example software or similar services, where a consumer can directly with his computer log into a service terminal, so-called server, study different softwares and perhaps buy a wanted software. This electronic distribution enables elimination of the drawbacks, but other problems rise.

One problem is to ensure that the consumer can order the product. There is no way for the consignor (selling) part to control that the data transmission has been complete. Disruptions in the connection occur frequently. The customer cannot risk the payment and see its delivery fail without being able to prove it. The result is that no secure trade can be carried out if the problem is not solved.

For a producer of software, there is a way of merchandising its software which has been placed

in a seller server, for digital selling. In this case, another problem for the software producer is to know how many softwares that the seller has sold or distributed.

DE-A1- 3938479 describes a system for transmitting, for instance software via a network between a first and a second computer software. The software consists of two programme portions, one part sends back an inquiry to the first computer for permission to use the software, which as a positive answer sends a key over to the second computer, which locks up the software for use.

Brief description of the invention

One objective of the present invention is to eliminate above problems and ensure for instance payment, distribution and sales report to possible supplier.

A further object of the invention is to provide an entirely novel method to practise trade with software products, which contributes to environmental savings, low costs, rapidity and possible positive cash flow, preferably without credits from the supplier or others.

These objects are obtained by the system described in the beginning, which is characterised by the server being arranged to produce a first encrypted and with a password-locked package of the specific data set, which password is generated at least partly based on the information received from the client station. Moreover, the server is arranged to produce a second package containing said first package and an instruction set, whereby at least parts of said second package can be accessed if the client station receives it in its entirety after a transmission. The encrypted data set further being provided to be accessed if the client station performs instructions acceptable by the distributor, which supplies the password for unlocking said first package.

Brief description of the drawings

The present invention will now be described in more detail under reference to an embodiment illustrated on the enclosed drawings.

Fig. 1 is a schematic view of a computer network,

Fig. 2 is a flow chart showing the steps according to the present invention, and
Fig. 3 is a schematic view of a transmission package, according to the invention.

Detailed description of an embodiment

The system, in its simplest form illustrated schematically in fig. 1, includes at least one service unit 10 or a server and one or more consumer stations 11, which are interconnected via some type of electrical link or network 12. The server 10 is directly or indirectly equipped with storage units for storing information and software to be distributed. The server 10 may also include different databases containing information about customers, products, price lists etc.

A consumer station 11 is connected to the server 10 via a network 12 by means of a modem or the like and besides suitable communication softwares does not need other special softwares to stablish contact with an appropriate server 10.

Fig. 2 shows the flow chart for the procedure when a contact is established and the communication between the server 10 and the station 11. The main object of the procedure is to generate a package 24 (fig. 3), substantially on request, containing the requested software 20 or other data 21, 22 in encrypted form and instructions, which can instruct to decode the encrypted information.

On request for purchase, the distribution procedure starts 100. The distribution procedure 100 requests 101 or automatically fetches necessary information about the buyer, for example name and electrical addresses, to which the order software should be delivered. The procedure waits 102, 103 until necessary information has been obtained. It is possible to check the buyer so that a buyer with poor credit rating is not allowed to buy the software. When correct information is obtained, a procedure 104 for generating codes to accompany the delivery starts. The code, which is called reference cod 21, includes, e.g. mainly information about the identity of the software which the customer has requested, date and the time for the transmission and the identity information. Then a password 105 is generated preferably from the reference cod according to a separate algorithm, for example by picking parts of information in the code or creating a special check sum, which is the basis for generation of the password. Obviously, other methods for generation of the password may occur. In each service 10, a reference file is

stored, which primarily includes buyer identity, an electrical delivery address and the reference cod generated according above. This reference file is updated 106 before transmission. Then a registration file 22 is generated 107, for example a text file intended for the buyer. The file also contains information to be re-transmitted to the supplier as well as information about the procedure for registering the software etc. Moreover, the file can contain a password or a unique identity cod, which corresponds to the supplier to control the authenticity of the file. A first electronic package, called the software package mainly containing the registration file 22 and the purchased software 20 as well as possible instruction documents 21 is created 108, packaged (preferably produced in a known way just as one file), encrypted and lucked with a password generated according to above description. At the next step an instruction file 23 is created 109, for example a text file, which among others contains instructions to the buyer about the payment procedure, licence conditions and the reference cod according above. This file is not encrypted and can be opened by the buyer. In the next stage a second package 24 is created 110, called the transmission package including the software package created according to stage 108 and the non encrypted instruction file 23.

Particularly, the second package 24 can be created through such a method, that if the package due to transmission is damaged or if no complete transmission is carried out, the readability of the instruction file is prevented. For this reason, a control of the check sum of the package or the like can be carried out. The package 24 is generated through recognizable techniques known for a person skilled in the art and therefore no closer description is provided.

The transmission package 24 is then transmitted 111 to the electronic address obtained from the customer and the procedure is terminated 112, but a second part of the procedure can be started, which waits 113 for payment from the buyer. The transmission is carried out in a known way over a modem or network/modem, for example through use of FTP (Filet Transmission Protocol), packet switching or the like.

The entire or parts of the transmission package 24 may as well be compressed and/or converted to a (self) executable program, which can be ran by at reception.

If the transmission has been performed correctly, the transmission file can be opened by the

buyer and the instructions in the non-encrypted part of the package, i.e. in the instruction file be displayed. The fact that the transmission file can be opened confirms that the transmission has succeeded and is complete, which becomes a transfer acknowledgement.

The buyer can then read the instructions and settle the payment according to the instructions to a payment receiver, for example a bank or the like, at the same time indicating the received reference cod and other possible identity cods, e.g. his address, if the indicated reference cod is wrong.

At the distributor site, the server waits 113 for a communication from the payment receiver (the bank), that the payment has been received as well as the reference cod. The server then controls its reference database and if a correct amount is paid, it generates (or fetches from a database) once again the password based on the reference cod corresponding to that specific software package and transmits it to the buyer's electronic address.

The buyer can now use the password to decrypt the purchased software and install it.

In one embodiment, the payment can be deducted directly from an account at the distributor, which is performed automatically when the instruction file is opened or a special code from the instruction file is sent back to the server. In this case, the server sends back the password as soon as acknowledgement from the instruction file has been received.

Furthermore, the system can be provided with security routines, which indicate that no payment has been received after a certain period, so that the distributor or other suppliers can control if the software is decrypted and opened in some other way.

The system can be provided with a report generator, which transmits a report to the software producer, for example including information about the sale per software unit with the password that is used. The password information makes it possible to provide self controlling reporting procedure. If the producer's system receives registration files with other password than the one reported by the system, according to invention, the reports from the system are assumed to be incorrect and further control may be performed.

As a further precaution the annual sale of sold softwares can be confirmed to the suppliers, for example from the bank after an audit from the company accountants.

The system according to the present invention facilitates different alternatives to reduce the failure intensity, which provides a safe and reliable system.

If no password is received from the system in spite of correct payment, the buyer may complain to the system by indicating the reference cod. The code is controlled in comparison to the reference file and even though it is missing but the code is correct (for example through creating a new code by means of date information in the reference cod) the system can send a new password, but if the code is invalid, the earlier is discovered and a reimbursement can be performed.

If the password does not work, i.e. the software package cannot be opened, the customer is asked to resend the software package to the system for control and a new package can be sent to the customer, if he is right; preferably, all steps are performed through electronic distribution.

If the customer by mistake deletes the software, the system may after verification of the accomplished purchase allow the customer to receive the password directly after a new transmission initiated by the customer.

While we have illustrated and described a preferred embodiment of the invention, it is obvious that several variations and modifications within the scope of the enclosed claims may occur.

The invention is neither limited to sale and purchase of software via Internet. The system can be used within different applications and different network solutions. The system can be used for secure transmission of data, for example between different computers where acknowledgement for transmitted correct data is required.

Furthermore, the data may consist of moving (video or the like) or still images, newspaper articles, music, currency transactions, purchase and distribution of books (a so-called paperback) or the like.

It is obvious for a skilled person that the steps according to the description may be varied or performed simultaneously.

DESIGNATION SIGNS

10	Service server
11	Consumer station
12	Network
20	Software
21	Reference cod
22	Registration file
23	Instruction file
24	Transmission package

CLAIM

1. A system for data transmission over an electrical link (12) including at least one distribution server (10) and one client station (11), which requests transmission of a specific set of data from a distributor, communicating with the distribution server (10),
characterised in,
that the server (10) is arranged to produce a first encrypted and with a password-locked package of the specific set of data, the password being generated at least partly based on the information received from the client station (11),
that the server (10) is provided to produce a second package (24) containing said first package and an instruction set, at least part of the second package being accessible if the client station (11) receives it in its entirety after a transmission, and
that the encrypted set of the data is further provided to be accessed if the client station (11) performs instructions acceptable for the distributor, and supplies the password for unlocking said first package.

2. The system according to claim 1,
characterised in,
that the server (10) is arranged to request transaction information from the client station (11) before a transaction,
that the server (10) by means of said transactions information fetches data to be transmitted to the client station (11),
that the server generates a reference cod, substantially based on the information received from the client station,
that the server (10) generates a first electronic package provided with the password consisting of the information set required by the client station and reference file,
that the server (10) generates a second preferably non encrypted package including the first package and an instruction file,
that the second package is transmitted to the client station (11), and
that after performing a correct action, the client is provided with a password for decryption of the first package.

3. The system according to any of claims 1 or 2,
characterised in,
that the electronic link is a computer network.

4. The system according to any of claims 1 or 2,
characterised in,
that said electronic link is Internet.

5. The system according to any of claims 1 to 4,
characterised in,
that the requested data set consists of software and possible corresponding instructions.

6. The system according to any of claims 1 to 5,
characterised in,
that second package (24) is produced as an executable file.

7. A method for data transmission over a network (12) including at least one distribution server (10) and a client station (11) requesting transmission of a specific set of data from a distributor communicating with the distribution server (10),
characterised in,
that the method includes the steps of: producing a first encrypted and with a password-locked package of said specific set of data, the password being generated at least partly based on information received from the client station (11),
producing a second package (24) containing said first package and an instruction set, at least part of said second package being accessible if the client station (11) receives it in its entirety after a transmission, and
making the encrypted data set accessible if the client station (11) performs instructions acceptable by distributor, which provides said password for unlocking said first package.

8. The method according to claim 7,
characterised in,
requesting transaction information from the client station (11) before a transaction,

fetching data to be transmitted to the client station (11) by means of the transaction information,
producing a reference cod, essentially based on information received from the client station,
producing a first electronic package provided with password and consisting of the information set requested by the client station and the reference file,
producing a second package, preferably not encrypted, including said first package and an instruction file,
transmitting said second package to the client station (11), and
providing the client station with the password for decrypting the first package after an approved action.

9. The method according to claim 7 or 8,
characterised in,
that the second package (24) is an executable file.

FIG.1

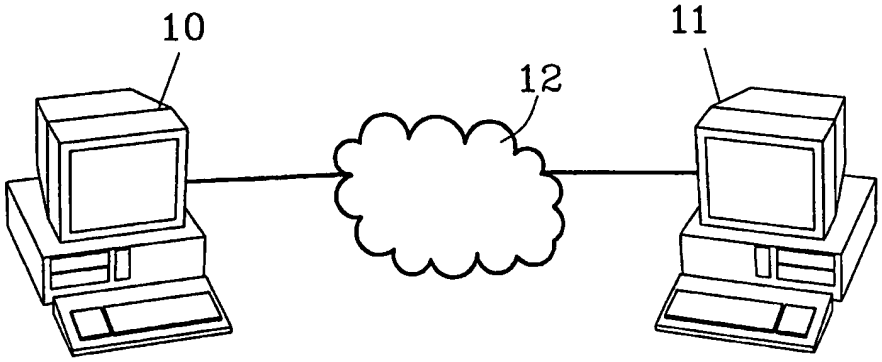


FIG.3

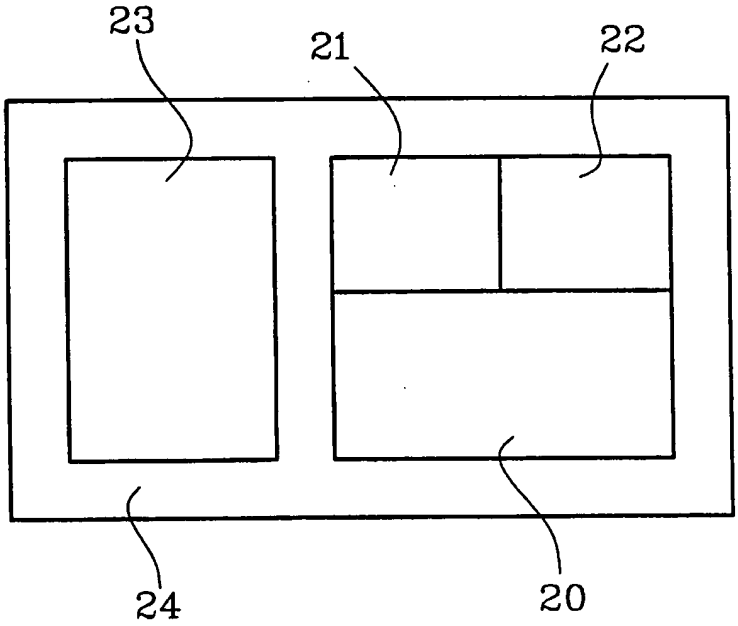
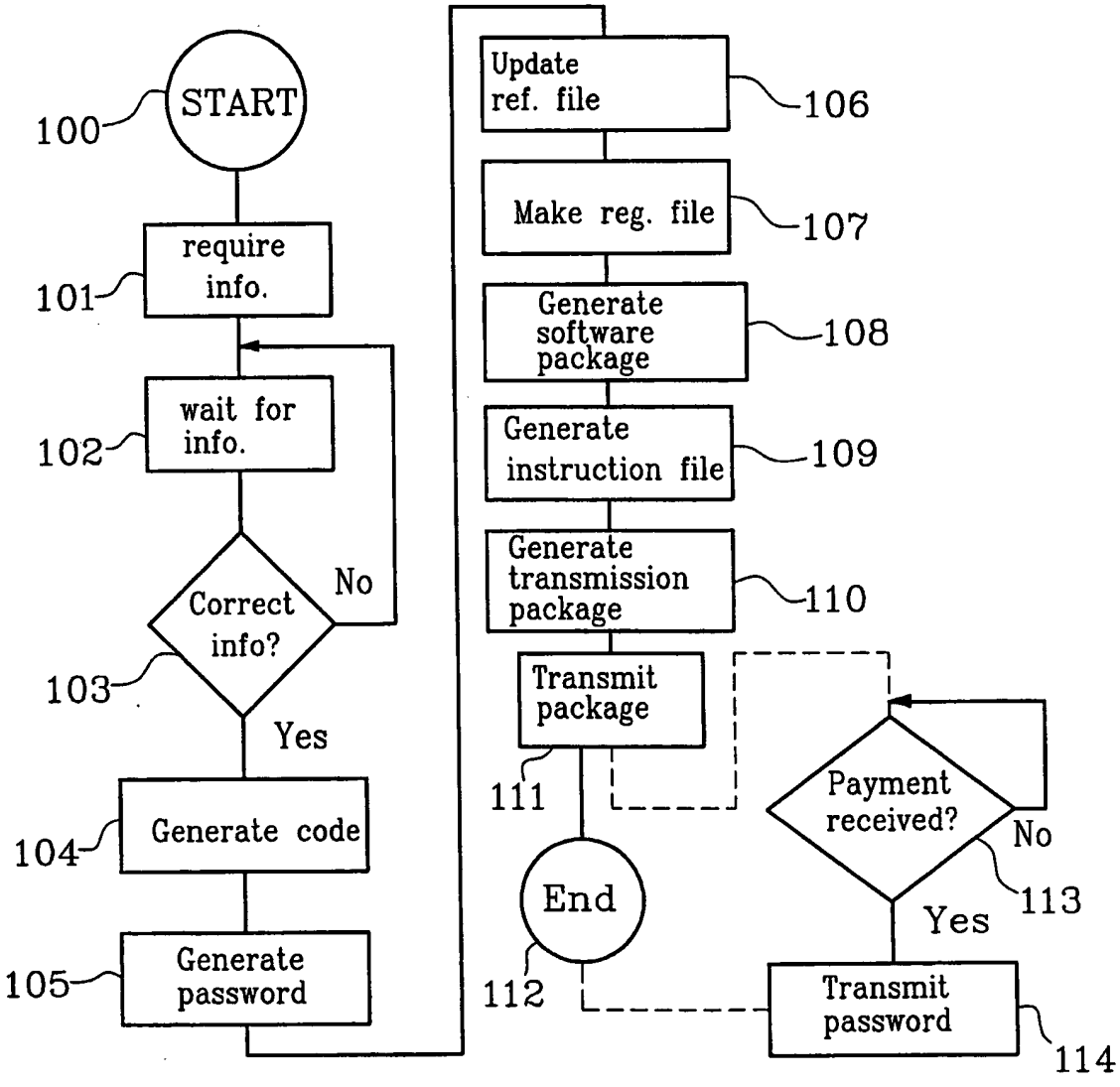


FIG.2


START
100
require info.
101
wait for info.
102
Correct info?
No
103
Yes
Generate code
104
Generate password
105
Update ref. file
106
Make reg. file
107
Generate software package
108
Generate instruction file
109
Generate transmission package
110
Transmit package
111
End
112
Payment received?
No
113
Yes
Transmit password
114